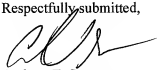
PRE-APPEAL BRIEF REQUEST FOR REVIEW (filed with the Notice of Appeal)	Docket Number 042933/294057
Application Number 09/944,694	Filed August 31, 2001
First Named Inventor Matthew Gast	
Art Unit 2135	Examiner Leynna A. Ha

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

Respectfully submitted,



Andrew T. Spence
Registration No. 45,699

Date August 5, 2008

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111
LEGAL02/30904602v1

Attachment

Reasons for Requesting Pre-Appeal Brief Request For Review
(no more than five 5 pages may be provided)

REMARKS/ARGUMENTS

These remarks are hereby filed concurrent with a Pre-Appeal Brief Request for Review, following a final Official Action dated February 5, 2008, and an Advisory Action dated May 22, 2008. The present application includes pending Claims 1, 2 and 4-11, all of which stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,032,242 to Grabelsky et al., in view of U.S. Patent No. 6,356,529 to Zarom. Applicant respectfully submits that the claimed invention is patentably distinct from Grabelsky and Zarom, taken individually or in any proper combination. In view of the remarks presented herein, Applicants respectfully request reconsideration and withdrawal of the rejections of all of the pending claims.

As previously explained, Grabelsky discloses a system and method for distributed network address translation with security features provided by Internet Protocol security protocol (IPsec). The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol (IP) address of a given local network device and a IPsec Security Parameter Index (SPI) associated with an inbound IPsec Security Association (SA) that terminates at the local network device. In a passage of Grabelsky cited by the Examiner, IPsec defines the security service Encapsulated Security Payload (ESP), and may be applied in a transport mode. In the transport mode, a sending endpoint may apply ESP to outbound packets in a manner including encapsulating information using a selected encryption technique (col. 23, ll. 27-39). Separately, a receiving endpoint may apply ESP to inbound packets in a manner including decryption using an encryption technique indicated by an appropriate security association (SA) (col. 23, l. 49 – col. 24, l. 4).

Zarom discloses a system and method for translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols. As disclosed, wireless communication devices that operate in accordance with WAP network protocols require a translation system, or gateway, to communicate with other devices that operate in accordance with IP protocols. Zarom therefore discloses a system and method for WAP translation in a manner that enables a gateway translator to perform the translation process as soon as a minimal portion of data has been received.

According to one aspect of the claimed invention, as reflected by independent Claim 1, a method for providing network security includes receiving a plurality of network protocol packets (e.g., IP packets). A network protocol packet includes a network protocol header (e.g., IP header) and a plurality of network protocol data, which includes a first cryptographic protocol header (e.g., TCP header) and a first plurality of encrypted data (e.g., SSL data). At least a portion of some of the network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP). As also recited, a first

plurality of cryptographic protocol rules (e.g., WTLS rules) associated with the network protocol data is determined, with a cryptographic session being established if required by the first cryptographic rules. The first plurality of cryptographic protocol rules are applied to the first encrypted data to obtain a first plurality of cleartext data (e.g., WML data). The first plurality of cleartext data is translated into a second plurality of cleartext data (e.g., HTML data) in accordance with at least one translation rule. The second plurality of cleartext data is then encrypted in accordance with at least one rule associated with a second cryptographic protocol (e.g., HTTP over SSL), resulting in a second plurality of encrypted data.

In contrast to the second aspect of the claimed invention, and as conceded by the Examiner, Grabelsky does not teach or suggest translating a first plurality of cleartext data into a second plurality of cleartext data. Nonetheless, the Examiner alleges that Zarom discloses this feature, and that one skilled in the art would have been motivated to modify Grabelsky to include the aforementioned feature of Zarom to teach the claimed invention. Applicant continues to disagree, however, and submits that even if Grabelsky and Zarom did disclose respective features of the claimed invention, one skilled in the art would not in fact have been motivated to modify Grabelsky to include the feature of Zarom to teach the claimed invention.

Applicant again notes that the Examiner cites a passage of Grabelsky directed to a receiving endpoint applying ESP to inbound packets, and alleges that this passage reads on the claimed feature of applying a first plurality of cryptographic protocol rules to first encrypted data to obtain a first plurality of cleartext data. The Examiner cites a passage of Grabelsky directed to a sending endpoint applying ESP to outbound packets, and alleges that this passage reads on the claimed feature of encrypting a second plurality of cleartext data into a second plurality of encrypted data. Then, the Examiner cites Zarom for disclosing a gateway translator translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols, and alleges that this passage reads on the intervening translation of the first plurality of cleartext data into the second plurality of cleartext data.

As previously explained, taking the Examiner's interpretation of Grabelsky and Zarom as a given (although expressly not admitted), the combination of Grabelsky and Zarom teaches a receiving endpoint decrypting first encrypted data into a first plurality of cleartext data, a gateway translator then translating the first plurality of cleartext data into a second plurality of cleartext data, followed by a sending endpoint encrypting the second plurality of cleartext data into a second plurality of encrypted data. To effectuate the security services of Grabelsky, it only makes logical sense that the functions attributed to the receiving endpoint, gateway translator and sending endpoint are all performed by a single entity between endpoints within different networks (and thus needing address translation), such as by the router of Grabelsky. As disclosed by Grabelsky, however, the router does not modify the contents of received, secured (IPsec) packets since to do so would compromise the security of those packets. *See* Grabelsky, col. 3, l. 54 – col. 4, l. 3; col. 25, ll. 31-34; col. 32, ll. 45-46. Thus, even given the Examiner's interpretation of Gravelsky and Zarom (again expresssly not

admitted) one skilled in the art would not be motivated to modify the end-to-end address translation with security of Grabelsky, with the translation of Zarom, to disclose the claimed invention.

In response to the foregoing, the Examiner notes that Grabelsky discloses overcoming the drawbacks of conventional network address translation (NAT) devices by implementing a distributed NAT (DNAT). Even considering Grabelsky's DNAT technique, and the alleged disclosure of Zarom, Applicant still maintains that one skilled in the art would not have been motivated to modify the router of Grabelsky to include any translation attributed to Zarom. The final Official Action continues to refer to passages of Grabelsky referring to prior art NAT techniques to assert that the disclosure of Grabelsky indicating that the router does not modify secured packets relates to the prior art NAT techniques and their drawbacks with respect to IPsec, and not the DNAT technique of Grabelsky. Applicant respectfully disagrees, however, and notes that at least at column 32, ***Grabelsky explicitly states that its router (router 26 of FIG. 1, "illustrating a network system for distributed address translation" – col. 5, ll. 35-36) "does not modify contents of a received IPsec packet."*** Grabelsky, col. 32, ll. 45-46 (emphasis added). And given the fact that Grabelsky explicitly does not modify the contents of a received packet so as to avoid compromising the security of that packet, one skilled in the art would not have been motivated to modify Grabelsky to translate a received packet, as alleged in the Official Action.

Applicant therefore respectfully submits that independent Claim 1, and by dependency Claims 4-11, is patentably distinct from Grabeksky and Zarom, taken individually; and respectfully submit that Grabeksky and Zarom cannot reasonably be combined to teach or suggest independent Claim 1, and by dependency Claims 4-11. Applicant also respectfully submits that independent Claim 2 recites subject matter similar to that of independent Claim 1. As such, Applicant respectfully submits that independent Claim 2 is patentably distinct from Grabeksky and Zarom for at least those reasons explained above with respect to independent Claim 1.

A. Dependent Claims 6 and 9

In addition to the aforementioned reasons, Applicant continues to maintain that various ones of dependent Claims 4-11 recite features that are further patentably distinct from Chang, Grabeksky and Zarom, taken individually or in combination. For example, dependent Claims 6 and 9 further recite that the first and second cryptographic protocols comprise WTLS and SSL over HTTP, respectively. The Official Action cites both Grabelsky and Zarom for allegedly disclosing the feature of Claim 6, citing column 7, lines 10-12 of Grabelsky and column 3, lines 5-6 of Zarom for disclosing WTLS; and cites Zarom for allegedly disclosing the feature of Claim 9, citing column 8, lines 7-11 for disclosing SSL over HTTP. Applicant respectfully submits, however, that not only do none of these passages disclose the features to which they are attributed, but no other passage of Grabelsky or Zarom disclose those features.